Testimony to Congressional Committee

September 13, 2006

APPLYING SYSTEMS ENGINEERING METHODOLOGY TO HELP SECURE AMERICA'S BORDERS

Testimony before the 109th Congress Hearing of the
Committee on Science
United States House of Representatives
Room 2318 Rayburn House Office Building
Washington, D.C.

on

"How Can Technologies Help Secure Our Borders?"

by

Gordon Daniel Tyler, Jr.
Department Head
National Security Technology Department
The Johns Hopkins University
Applied Physics Laboratory

This page intentionally left blank.

EXECUTIVE SUMMARY

Significant investments in securing our Nation’s borders over the last decade have not produced capabilities that met operational expectations. The issue for developing systems and operations that address this massive, technically complex, and time critical challenge is identifying an approach to systems development that has a high likelihood of success. Notably, the collective experience of a rich history of producing complex engineered systems has been assimilated into a methodology with a proven track record of achievements——systems engineering.

The systems engineering methodology provides a disciplined approach to requirements, concepts, planning, prototyping, testing, and other elements of system development and operational deployment. Systems engineering mitigates risk, controls cost, and ensures performance when prompt responses to exigent challenges are needed. In particular, the systems engineering methodology can provide the oversight tool that helps Congress and the Department of Homeland Security (DHS) monitor the progress of the Secure Border Initiative (SBInet) with metrics and guide its ultimate success. In times of tight budgets and the need for urgency, as in today’s volatile national security environment, it is tempting to abandon the rigor and discipline of systems engineering in favor of ways of doing business that appear less expensive and more rapid . Repeatedly, these other formulas have fallen short of the mark, producing activity without real progress, while systems engineering has a history of delivering performance, on budget and schedule. The systems engineering methodology has been institutionalized in standards and policy by virtually all acknowledged professional technical societies and Government agencies for the development of massive, complex systems.

While adopting the systems engineering methodology is essential for engineering large-scale, highly complex systems, special attention must be paid to employing an implementation strategy that ensures adherence to the principles of systems engineering, and successful execution

of its various phases. The Government is ultimately accountable for results, and must ensure adequate Government technical competence is brought to bear for understanding issues and making decisions. When needed, especially with complex problems, the Government may engage 3rd party organizations to support them in this capacity.

The systems engineering discipline is not prescriptive regarding implementation strategies, and there are assorted successful examples. The Navy’s management of the the Polaris Program, initiated in 1956, included a technical staff of 450 in the Program Office fully dedicated to the development and production of the Polaris system. The Navy’s sonar development program started in 1996, relies heavily on the broad technical community, operating in peer working groups, for concept identification, feasibility assessment, prototyping, and especially for validation and testing at every phase of the systems engineering methodology. For each system development activity, specific consideration should be given to the appropriate roles for Government agencies and Government laboratories, prime contractors, associate contractors, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, nonprofits, and small or minority owned businesses. In architecting an implementation strategy, especially in defining the roles of prime contractors, note that history has shown that the strength of this Nation for addressing massive, complex challenges is the wealth of available domain expertise, and the power of competitive forces.

The systems engineering methodology is flexible. It can be tailored to emphasize risk mitigation, incremental improvement, capability-based acquisition, as well as milestone- or cost-driven development. Given the urgency of the current national security environment, a particularly relevant issue is how to make real and rapid progress: How much can we improve operational effectiveness and how long will it take? The Secure Border Initiative program component (SBInet) has existing advantages for getting underway quickly: i.e., current Integrated Surveillance Intelligence System (ISIS) sensors, video surveillance, and infrastructure; an imminent Indefinite Delivery, Indefinite Quantity (IDIQ) prime contract; very promising technology in the pipeline; and data that can be used to address technical issues and support technology development. The program now needs to adopt a disciplined systems engineering methodology, and demonstrate a successful, limited-deployment operational system, conceivably within two years, before going into full production and deployment.

This page intentionally left blank.

CONTENTS

LIST OF ACRONYMS

APB	Advanced Processor Build
ARCI	Acoustic Rapid COTS Insertion
ASI	America's Shield Initiative
AT&T	American Telephone and Telegraph
BPOE	Between Ports of Entry
CBP	Bureau of Customs and Border Protection
CNO	Chief of Naval Operations
CONOP	Concept of Operations
COTS	Commercial Off-the-Shelf
DHS	Department of Homeland Security
DOD	Department of Defense
DOE	Department of Energy
DOT&E	Director of Operational Test and Evaluation
FBM	Fleet Ballistic Missile
FFRDC	Federally Funded Research and Development Center
GAO	Government Accountability Office
GAO	General Accounting Office
GSA	General Services Administration
HUMINT	Human Intelligence
ICAD	Integrated Computer Assisted Detection
IDIQ	Indefinite Delivery, Indefinite Quantity
IEC	International Electrotechnical Commission
INS	Immigration and Naturalization Service
ISIS	Integrated Surveillance Intelligence System
ISO	International Organization for Standardization
OA	Open Architecture
OBP	Office of Border Patrol
OIG	Office of Inspector General
ONR	Office of Naval Research
PDA	Personal Digital Assistant
PEO	Program Executive Office
POE	Ports of Entry
RFP	Request for Proposals
RVS	Remote Video Surveillance
S&T	Science and Technology
SBI	Secure Border Initiative
SBInet	Secure Border Initiative (Program Component)
SSP	Strategic Systems Programs
TEASG	Test, Evaluation, and Support Group
UARC	University Affiliated Research Center
UAV	Unmanned Aerial Vehicle
USD (AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics

MAIN TESTIMONY

Chairman Boehlert, Congressman Gordon, and members of the House Committee on Science. I am G. Daniel Tyler, Head of the National Security Technology Department at The Johns Hopkins University Applied Physics Laboratory (JHU/APL). Thank you for the opportunity to address you today on "How Can Technologies Help Secure Our Borders?" The Applied Physics Laboratory has been a long-term, trusted strategic partner with the Federal Government, in particular the Department of Defense (DOD) and the Navy, for providing critical contributions to our Nation's most pressing national security challenges. I am pleased to be able to share our insights with the committee as to the applicability of a disciplined systems engineering approach to the elusive challenge of securing our Nation's borders.

PREFACE

What is systems engineering? Other areas of engineering (e.g., electrical, mechanical, chemical, etc.) are considered "disciplines" in that they are fields of study, and spheres of domain expertise. More prescriptive are "processes" that define the steps or tasks to be executed conducing to an end. Systems engineering is a discipline, less regimented than a well-defined process, best described as a methodology. In particular, systems engineering is defined by a set of phases with associated activites that must be performed. If these activities are absent, then the systems engineering methodology is not being followed.

The traditional systems engineering methodology for designing, developing, and deploying major systems is usually described in three phases:

1. **Concept Development** – needs, feasibility, requirements, concept definition, and detailed planning
2. **Engineering Development** – prototyping and testing for operational use
3. **Post-Development** – production, deployment, operations, effectiveness assessment

In times of tight budgets and urgency driven by a volatile national security environment, it is tempting to look for ways of acquiring needed capabilities that appear to be less expensive and more rapid. A reasonable question is: Are the rigor and discipline of the systems engineering process really necessary for developing appreciably complex systems? The foreman on a jobsite constructing a new home may be able to manage the entire construction process, plan, and schedule in his head, and single-handedly coordinate contractors. In contrast, consider the program manager responsible for the construction of an aircraft carrier, clearly dealing with more complexity than a single human brain can accommodate at once. Major system development efforts are usually complex, need to support specified user requirements, are composed of many interrelated tasks, involve several different disciplines, are performed by multiple organizations, have a specific schedule and budget, and may require years to complete. The human brain can conceptualize and manage small development activities, but larger efforts demand a disciplined process. The issue is identifying a process that, in some sense, optimizes the probability of success for developing a complex system, while mitigating risk and controlling cost and schedule.

SYSTEMS ENGINEERING AND SBI/SBINET

The Secure Border Initiative (SBI) and SBInet are large, complex system solutions to an immediate critical challenge facing our Nation. Properly applying the systems engineering methodology to the challenge of securing our borders makes sense because:

- A disciplined systems engineering approach can develop and deliver massive, complex systems with a proven high rate of success.
- Previous approaches to securing our country’s borders have not met operational expectations, according to the GAO and other testimony.

- The systems engineering methodology provides the right tools for oversight and success: i.e., requirements, metrics, planning, prototyping, testing, and deployment for operational use.
- Both the public and private technical and acquisition communities have embraced systems engineering and shown its effectiveness for controlling performance, schedules, and cost.
- Organizationally, implementing a systems engineering process properly requires appropriate roles for the Government and Government laboratories, prime contractors, associate contractors, independent laboratories, and academia.

There is a profound difference between mere activity and progress. There are easy ways to simply take action, but systems engineering is the way to ensure progress. Applying a disciplined, deliberate systems engineering methodology to the border security challenge provides a proven development process for controlling performance, budgets, and schedules. Moreover, the systems engineering methodology provides an oversight tool to help Congress and the Department of Homeland Security (DHS) monitor the progress of SBInet with metrics and therefore guide its ultimate success.

DELIVERING MASSIVE, COMPLEX SYSTEMS WITH PROVEN SUCCESS

The Nation has a rich history of relevant experience in successfully developing massive, engineered systems:

- Investing $50B in converting the Nation's telecommunications infrastructure from analog to digital;
- Going to the moon in less than a decade;
- Integrating three major and diverse weapons systems from two services with global command, control, and communications, and providing interfaces with the

Intelligence Community and the White House to realize a Strategic Deterrence system of systems.

We even have experience, similar to the border security challenge, in more than one mission area, for providing surveillance over large geographic areas and supplying cueing for follow-on forces. Between 1950 and 1985, for example, in support of the Anti-Submarine Warfare mission, the Navy's surveillance community successfully produced a system that provided surveillance and cueing for 12,000,000 square nautical miles of ocean, including 20 worldwide Naval Facilities for shore-based processing and analysis and thousands of Navy and civilian support personnel.[1]

Previous efforts have tackled the same types of issues facing the border security challenge. Historically, in the development of large and complex systems it has been the norm that at the outset, designers could readily identify many technical issues to address; however, there have also been "unknown unknowns" that surfaced only during the phases of development and testing. Critical system elements may have been nonexistent and required rapid directed research to produce seemingly miraculous results. Prior system development efforts necessarily had to deal with the problem of balancing technology against human resources. Concepts of Operations (CONOPS) had to be developed. Often, the total solution for a successful mission required addressing a myriad of issues under the jurisdiction of multiple agencies. However, lessons have been learned in the design, development, and deployment of these major systems that clarified what processes, management structures, and assignment of organizational roles and responsibilities were most effective for realizing acceptable system performance, controlling cost, and attaining operational capability as rapidly as possible. The modern discipline of systems engineering has assimilated this collective experience into a proven process.

[1] Edward C. Whitman, "The Secret Weapon of Undersea Surveillance," Undersea Warfare, Winter 2005, Vol.7, No.2.

An example that Congress is familiar with is the Navy's Fleet Ballistic Missile (FBM) Program. This program has been so widely recognized and studied as a DOD acquisition success story, that in 1990, the General Accounting Office (GAO) produced a report[2] for Congress to clarify what made this program so successful. The Navy initiated the program in December, 1956, when it began development of a submarine-launched ballistic missile (Polaris) under a new organization, the Special Projects Office [now called Strategic Systems Programs (SSP)]. SSP was given complete authority to design, develop, produce, and support the FBM system.

> "Three major components – a solid propellant fuel, a small high yield nuclear warhead, and an accurate guidance/fire control/navigation system – needed major technical breakthroughs at the time that the Polaris project was authorized. A nuclear attack submarine also had to be modified to carry and launch the missiles while submerged."

The first Plans and Programs Director of SSP made the analogy that,

> "…building and fielding Polaris was similar to building the entire automobile industry. That is, not only did the first automobile have to be developed but also the internal combustion engine, tires, the oil industry, gas stations, and driver training before the automobile's feasibility was known."[3]

Amazingly, the technical problems were solved, and "the Polaris program went from concept development to deployment in 3 years —3 years ahead of the original schedule." Between 1956 and 1990, about $74B was appropriated for FBM program acquisition. Three classes of FBM submarines have been deployed (59 hulls), and six generations of missiles (more than 3000 missiles). A key

[2] United States General Accounting Office, "Fleet Ballistic Missile Program," GAO/NSIAD-90-160, 9-6-1990.

[3] Ibid.

finding of the GAO study is the commitment over the entire lifecycle of the system, for the following:

“(1) concept exploration/definition,
(2) concept demonstration/validation,
(3) full-scale development and low rate initial production,
(4) full-rate production and initial deployment, and
(5) operations support”

(coincidentally, all of the components of the systems engineering paradigm).

Importantly, SSP’s implementation of systems engineering relies strongly on independent test and evaluation in all phases of the process.

The message from the FBM program and history is clear. We have engineered many large, complex, technology-based systems, comparable in scale to the challenge of securing our borders. We have learned a lot from employing different development processes and from our successes and failures. We have developed a sense for what works and what does not work. Although there is no guaranteed “cookbook” approach to developing massively complex systems, there is a high correlation of success with employing a disciplined systems engineering development process.

THE CURRENT INABILITY TO MEET OPERATIONAL EXPECTATIONS

Some of the challenges in securing our Nation’s borders are obvious: 10,000 miles[4] of diverse land borders and coastline and 1.5 million illegal aliens yearly[5] present formidable impediments to gaining control of our borders. Solutions whose core attribute consists of employing large quantities of sophisticated technology and significant

[4] Does not include Alaska or Hawaii.

[5] Source: “Estimates of the Unauthorized Migrant Population for States Based on the March 2005 CPS,” Pew Hispanic Data Center Fact Sheet, 26 April 2006. Estimate is based on U.S. Census Data; estimate of 1.5M illegal aliens per year since 2000.

human resources (e.g., border patrol agents), may have an intuitive appeal, but this is in the absence of a deeper understanding of more subtle, qualitative, and complex performance drivers. This appears to be the case in the recent history of attempts to improve border security. Starting in the 1970s and 1980s, the Office of Border Patrol (OBP) introduced acoustic and magnetic sensors and video cameras to assist agents in remotely detecting illegal aliens entering the United States. In 1998, the Immigration and Naturalization Service (INS) formally established the Integrated Surveillance Intelligence System (ISIS) comprising more than 11,000 seismic and magnetic sensors, 255 operational remote video surveillance (RVS) systems, and the Integrated Computer Assisted Detection (ICAD) system. In 2003, OBP recognized the need to further improve border surveillance and remote assessment and monitoring technology, due to poor program management, technology failures, and poor operational results for ISIS[6]. Therefore, OBP began developing the America's Shield Initiative (ASI). This initiative included additional surveillance structures, upgraded and expanded surveillance equipment, and significantly enhanced detection and monitoring capabilities. According to OBP, the expanded use of surveillance technologies was viewed as an effective force-multiplier. In an April 7, 2006 hearing of the House Appropriations Subcommittee on Homeland Security, the opening statement of Chairman Harold Rogers summarized real progress over this time period:

> "Since 1995, we have quadrupled spending on border security, from $1.2B to $4.7B, and more than doubled the number of Border Patrol Agents from 5,000 to 12,381; yet during that same time period, the number of illegal immigrants in the U.S. has jumped from 5 million to over 11 million."

We have applied significant resources, financial and human, to this challenge and still have limited control over

[6] Office of the Inspector General, DHS, "A Review of Remote Surveillance Technology Along U.S. Land Borders," OIG-06-15, December 2005

our borders. If we cannot deter or detect and stop illegal immigration, then we have no ability to stop terrorists using the same methods from infiltrating the U.S.

The massive scope of the border security issue deriving from large geographic areas and high volumes of illegal alien activity, is also technically challenging, operationally complex, and programmatically and contractually demanding for Government managers. In addition, it possesses multiple dimensions that interact in complicated ways, necessitating tradeoffs. In a December 2005 report[7], the Office of the Inspector General (OIG) of the DHS reviewed existing remote surveillance technology employed along U.S. land borders. This report contains valuable insights into some of the difficulties associated with attempts to exploit technology as a major contributor to border security operations. The following findings, organized by category, are from the OIG report's Executive Summary, which highlights technical, system, operational, and programmatic/contractual challenges:

Technical Challenges:

- "Remote video surveillance cameras do not have detection capability regardless of whether they are used in conjunction with sensors."
- "Current sensors cannot differentiate between illegal alien activity and incidental activations caused by animals, seismic activity, or weather …"[8]

System Challenges:

- "Integrated Surveillance Intelligence System (ISIS) components are not fully integrated: e.g., when a sensor is activated, a camera does not automatically pan in the direction of the activated sensor."

[7] Ibid.

[8] Nonsensor alerts along the southwest border during a five-day period generated by camera detections, vehicle stops, officer observations, other agency observations, citizen observation, air observation, or some other source totaled 780 alerts, resulting in 382 apprehensions. Over the same period, ISIS sensors generated 29,710 alerts, resulting in 252 apprehensions.

- "Data entered into OBP's primary source of ISIS information, the ICAD system, is incomplete, and not consistently recorded by OBP sectors."

Operational Challenges:

- " … OBP agents are often dispatched to false alarms."
- "OBP was unable to quantify force multiplication benefits of remote surveillance technology."
- "ISIS remote surveillance technology yielded few apprehensions as a percentage of detection, resulted in needless investigations of legitimate activity, and consumed valuable staff time to perform video analysis or investigate sensor alerts."

Programmatic/Contractual Challenges:

> "Deficiencies in the contract management and processes used to install ISIS equipment have resulted in more than $37 Million in DHS funds remaining in General Services Administration (GSA) accounts; delays in installing, testing, and bringing on-line RVS sites that are operational; and 168 incomplete RVS camera sites."

The OIG report concludes with helpful recommendations for addressing some of the identified deficiencies in the existing system and development process.[9] Justifiably, the OIG did not accept the charter, nor claim subject matter expertise for actually determining how an operational system could be engineered to provide adequate performance for meeting border security requirements. That is:

1. The OIG recommendations did not attempt to address specific technical solutions to problems (e.g., false alarm rates).

[9] The DHS OIG report spells out seven recommendations dealing with system integration, processes for handling data, performance measures, contracting issues, site selection, the use of Government and private structures, and mobile surveillance platforms.

2. Following the OIG recommendations may not be sufficient to produce a fully functional capability.
3. The OIG report was intentionally limited in scope (i.e., remote surveillance technology) and did not incorporate other critical elements of the problem.

Therefore, while the OIG addressed certain issues that stayed within the scope of its tasking, *a disciplined systems engineering review of ISIS/ASI would have provided a better baseline upon which to build a superior follow-on system – SBI/SBInet – to position it for success.*

The DHS OIG looked specifically at remote surveillance technology. While solving the technical problems here will clearly be a major move forward, other dimensions to this challenge need to be addressed before a viable concept can be realized for securing the borders. Importantly, these other elements interact, require interfaces, and necessitate tradeoffs that impact responsibilities and resource requirements across the boundaries of multiple agencies.

MULTIPLE DIMENSIONS OF THE BORDER SECURITY CHALLENGE

Fundamental tradeoffs need to be made between technology and human resources. Technology is easily envisioned as a force multiplier, but the experience with the current ISIS system testifies to the pitfalls in ignoring the technical details. The high false alarm rates associated with the currently deployed seismic/acoustic sensors drain the supply of additional OBP agents assigned to border patrol operations, producing a net decrease in operational performance. Synergism between technology and human resources needs to be carefully engineered, with a thorough understanding of the capabilities, limitations, and demands of the technology. In fact, technical solutions may burden human resources by affecting operations negatively and by requiring human interaction in controlling, operating, maintaining, and repairing technology and analyzing and communicating its products.[10] Significantly, the marriage

[10] ISIS operations require three types of personnel: law enforcement communications assistants for monitoring cameras and ICAD terminals

between technology and humans is not adequately defined until a CONOPS is developed that thoroughly defines how the technology and human resources will be jointly used operationally.

In addition to the technical, operational, and programmatic challenges, consider the impact of U.S. immigration policy on concepts for securing the borders. Nonrestrictive policy may focus attention on verification and inspection at ports of entry (POE). Conversely, restrictive policy will probably result in large numbers of illegal aliens attempting to enter between ports of entry (BPOE)—in deserts, forests, and mountainous regions—keeping attention on surveillance systems, border patrol operations, and detention facilities. Decision makers need to be fully cognizant of the impact of policy on the viability, cost, and schedule of any solution to this problem. Moreover, system developers must recognize that policy is a major driver in system design.

The threat itself is another dimension to the problem that must also be taken into account. The threat is not monolithic: It is composed of illegal immigration for economic and/or political reasons; trafficking in drugs, weapons, contraband, and human beings; and terrorism. The tactics employed may be different, the determination and persistence uneven, the level of desperation unpredictable, and the resources (financial, weapons) biased in favor of the most dangerous elements. We must fully account for the threat's ability to respond to our efforts and actively pursue countermeasures. As an OBP official observed, "Once illegal aliens learn where RVS camera sites are located, they may choose not to cross at those locations."

The troublesome part of the problem is that many agencies are involved, at the border and in the "interior" operations. Federal and state agencies can provide critical intelligence information and actively participate in border security operations. In addition, decisions made at the border will

and providing radio and dispatch support to field agents; OBP agents to respond to alerts, install and maintain cameras, and monitor sector RVS cameras; and CBP Office of Information Technology specialists for on-site repairs to sensors and cameras.

impact federal, state, and local agencies dealing with immigrant monitoring, verification of status and employment, and apprehension.

We can design a system focusing on technology and catching people at the border, or we can take a more holistic approach to the problems of illegal immigration, trafficking, and terrorism. Working all dimensions to the border security challenge collectively requires system engineering at multiple levels. A good example of this was the revolution in the telecommunications industry during the 1970s and 1980s. AT&T developed a three-tiered systems engineering approach for converting the Nation's telecommunications infrastructure from analog to digital:

1. Tier 1, the highest level, engineered the overall network, including local access, central switching, routing, long haul transmission, and other requirements.
2. Tier 2 system engineered each of the Tier 1 components addressing capacity, reliability, calling patterns, service views (e.g., 800/900 number services, calling cards).
3. Tier 3 system engineered specific technical systems (e.g., frame relay switches, fiber-optic networks).

A study of the AT&T experience, which required $50B over two decades, shows how multi-tiered systems engineering can be applied to the border security challenge: taking into account tradeoffs between humans and technology; addressing operations at ports of entry, between ports of entry, and in the interior; and devising a high-level construct encompassing roles for federal, state, and local agencies.

In summary, our attempts to date for improving border security through the exploitation of technology combined with operations have not met expectations or success. The problem may seem daunting – highly variable and massive in extent geographically, technically challenging, operationally complex, and possessing multiple dimensions that require sophisticated planning, coordination, and interfacing across organizational boundaries. Accepting that there are significant shortfalls in our current response to border security, as recognized by both Congress and DHS, the issue is where to go from here.

THE SYSTEMS ENGINEERING METHODOLOGY APPLIED TO BORDER SECURITY

Numerous paradigms exist for developing, producing, and operationally deploying technology and systems. Consider the "Linear Model" championed by great scientists like Vannevar Bush[11] and famous leaders like Franklin Roosevelt. This model starts with basic research then follows a progression through applied research, development, up through production and operations. This model pursues "discovery" first, then looks for application. It is a model used very successfully by many academic organizations, the Department of Energy (DOE) National Labs, and the services' research laboratories [e.g., the Office of Naval Research (ONR)]. When Government funds are used for the linear model, it is not necessarily known beforehand what will be discovered (if anything) or what utility any discovery might produce. At the other extreme, the Government can procure technology and systems for which there are no unknowns that need to be resolved, and which require only straightforward engineering to design and produce. Because national security involves known problems that need to be solved, with issues that frequently tend to be technically complex and massive in scale; because there has been an explosive growth in technology since the second half of the twentieth century; and because there is a continuing need to advance technology to pace the threat, neither the linear model nor straightforward procurement can successfully address many of the Nation's security challenges. The systems engineering method was specifically developed to meet this need.

[11] Vannevar Bush, "Science, The Endless Frontier," *Time Magazine*, April 3, 1944.

Kossiakoff and Sweet[12] define the characteristics of a system whose development, test, and application require the practice of systems engineering:

1. Is an engineered product and hence satisfies a specified need,
2. Consists of diverse components that have intricate relationships with one another and hence is multidisciplinary and relatively complex,
3. Uses advanced technology in ways that are central to the performance of its primary functions and hence involves development risk and often relatively high cost.

The development of a system for securing the Nation's borders easily meets these criteria and logically needs the deliberate application of a disciplined systems engineering methodology to succeed.

The systems engineering paradigm described here is based primarily on the text of Kossiakoff and Sweet[13]. While specific excerpts from this reference are quoted, the majority of ideas, concepts, and examples in this section are liberally based on material from the reference. Implications of the systems engineering methodology for the challenge of securing the Nation's borders, and examples based on existing deployed systems (ISIS/ASI), are provided in italics.

As mentioned in the Preface, systems engineering is usually partitioned into three phases:

1. **Concept Development** – needs, feasibility, requirement, concept definition, detailed planning
2. **Engineering Development** – prototyping and testing for operational use
3. **Post-Development** – production, deployment, operations, effectiveness assessment

[12] Alexander Kossiakoff and William N. Sweet, *Systems Engineering, Principles and Practice*, John Wiley and Sons, Inc., 2003.

[13] Ibid.

Concept Development Phase. This phase first establishes a need for the system and ensures that it is technically and economically feasible. Establishing the need typically requires analysis, modeling, and simulation for both the system and its operational employment. Technical feasibility generally requires that supporting science and technology necessary for developing viable system concepts are "in the pipeline." If a gap exists in a critical technology area, directed Science and Technology (S&T) may be needed, which increases the risk in system development.The second part of this phase explores potential system concepts and then formulates a formal set of requirements the system must meet. The importance of requirements is simply stated: If requirements are minimal, it will be easy for any system to meet them. Allowing contractors to establish requirements to encourage innovation and shorten acquisition cycles under OSD's acquisition reform did not work well.[14] Last, a viable system concept is selected, its functional characteristics defined, and a detailed plan is developed for the subsequent stages of engineering, production, and operational deployment of the system.

> *Requirements for securing the border need to be defined for the combined use of technology and border patrol agents. Choice of an appropriate metric is important: It affects system design, and its sensitivities may be subtle. For example, consider as metrics the success rate for illegal entry, the absolute number of illegal entries in a given period, and the number of illegal immigrants in the U.S. at any given time. Improving border security will have a direct, positive impact on all three metrics. Improved security may additionally have a deterrent effect on those considering attempting to enter illegally. The first metric is not sensitive to this deterrence, while the last two are. Additionally, observe that the first two metrics are principally under the control of the system designer, while the*

[14] Michael W. Wynne, Under Secretary of Defense (AT&L), "Policy for Systems Engineering in DOD," February 20, 2004.

last metric is heavily dependent upon other federal, state, and local agencies.

Once a Concept of Operations is developed for interfacing humans with technology, requirements can be established for communications and technology in the field: e.g., Personal Digital Assistants (PDAs), decision aids, and reachback (e.g., terrorist databases from the National Counterterrorism Center).

Numerous other technical issues arise in the concept development phase. Examples include: the existence of models, simulations, and analytical techniques for addressing the combined performance of systems and border patrol agents; the detection performance for sensors and cameras; system false alarm rates; potential Unmanned Aerial Vehicle (UAV) sensor contributions; the impact of law eneforcement human intelligence (HUMINT) on cueing, detection, and response.

Engineering Development Phase. This phase corresponds to the process of engineering the system to perform the functions specified in the system concept defined in the first phase. First, any new technology the selected system concept requires must be developed, and its capability to meet requirements must be validated. Second, a prototype is developed that satisfies requirements on performance, reliability, maintainability, and safety. Third, the system is engineered for production and operational use, and its operational suitability is demonstrated. These last two stages require engineering development and design, defining and managing interfaces, developing test plans, and determining how discrepancies in system performance uncovered during test and evaluation should be rectified.

Assuming that valid system requirements for border security and a system concept exist [while noting that the SBInet Request for Proposals (RFP) provided minimal requirements], gaps in critical technologies must be identified and addressed. Using the system concept for the current operational system (ISIS/ASI) as an example, critical missing technologies may *include: false alarm reduction algorithms; automation/semi-automation of the detection process for sensors and video, including "Bell Ringers" that alert operators and Large Margin Classifiers; algorithms for fusing acoustic, magnetic, video, and other sensor information; creation of a common tactical scene; tactical decision aids; Unmanned Aerial Vehicle (UAV) technologies including sensors, Automatic Target Recognition,autonomous operations; integrated C^2, man/machine interface, and law enforcement and intelligence interfaces.*

Prototyping of individual system elements must be completed and performance validated through testing (e.g., are we really achieving acceptable false alarm rates from sensors?). A scaled prototype of an integrated system must be developed and tested in an operational environment with border patrol agents. Full-scale production and deployment should begin only after any discrepancies are resolved.

Post Development Phase. This last phase includes production, operational deployment, in-service support and engineering, and continuing assessment of the operational effectiveness of the system, with feedback to prior phases and iterations as required to maintain/improve system effectiveness ("Build-Test-Build").

Full-scale production of complex systems for providing border security is appropriate only after the system successfully undergoes operational test and evaluation. Once deployed, it is critical to determine the operational effectiveness of the system, establishing whether the system is meeting its operational requirements, and understanding discrepancies and actions needed to be taken. There is a potential wealth of information from a deployed system for addressing deficiencies and improving system effectiveness: e.g., recorded sensor data; captured performance for the combination of the analyst and system for detecting targets and eliminating false alarms; empirical understanding *of the utility of command, control, and communications; the success of the marriage between technology and Bureau of Customs and Border Protection (CBP) operations. Given the lack of maturity of this mission area and the associated absence of subject matter expertise in critical technical areas (e.g., target signatures, false alarm mechanisms for sensors), a "Spiral Development" process of system capabilities could be entertained that would exploit the continually improving knowledge in this domain.*

Systems Engineering a Complex System with Predecessor Technology

Descriptions of systems engineering usually appear to imply that a new system is being designed from scratch, with no regard for current systems that may have applicability. Existing systems will affect development of a replacement system in three ways:

1. Deficiencies of the existing system are recognized and may represent the driving force for a new design.
2. If deficiencies are not as serious as to make the current system worthless, the existing overall concept and functional architecture may constitute a good starting point for exploring alternatives.
3. Relevant portions of existing systems may be used in new designs, reducing risk and saving costs.

   Given the significant investment in the current ISIS and ASI systems (including seismic and magnetic sensors, RVS, and ICAD), it is desirable to seriously entertain the employment of these assets in future system designs.

PEDIGREE OF THE SYSTEMS ENGINEERING METHODOLOGY FOR CONTROLLING PERFORMANCE, SCHEDULES, AND COST

The systems engineering method basically consists of defining requirements, translating those requirements into functions (actions, tasks) that the system must accomplish to meet the requirements, selecting a preferred system design that is believed to accomplish those functions, then iterating and validating the system design through successive testing. If one views each iteration as a "hypothesis" that this design will optimally meet requirements, with associated "hypothesis testing" to verify this assumption, then "the systems engineering method can be thought of as the systematic application of the scientific method to the engineering of a complex system."[15] This is certainly not a rigorous proof that system engineering is an optimal method for developing complex systems, but it is a compelling rationale that appeals to the same logic that supports the scientific method for pursuing research. Would a legitimate researcher pursue discovery and invention without using the scientific method?

The systems engineering methodology has gained acceptance in virtually all acknowledged professional technical communities for the development of massive, complex systems. Figure 1, adapted from Kossiakoff and Sweet, shows the relationship between the elements of systems engineering as described here, to other prominent systems engineering life cycle models.

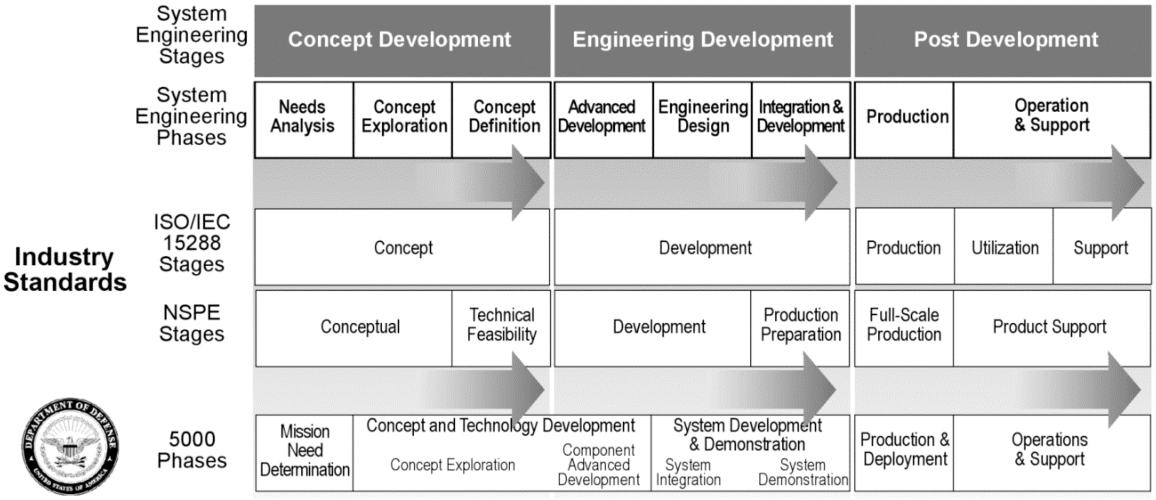

Figure 1 Comparison of system life cycle models.

[15] Ibid.

Consider the extensive experience realized by the United States during the twentieth century in developing large-scale, complex military systems (ships, tanks, planes, command and control). The Department of Defense developed the DOD 5000 series of directives as a set of comprehensive system acquisition guidelines, specifically to

> "…manage the risks in the application of advanced technology, and to minimize costly technical or management failures. … In 2001, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) issued the result of several years of effort – a systems engineering standard designated ISO/IEC 15288. This model is likely to become institutionalized in U.S. industry to replace previous standards.[16]"

As an additional example, the National Society of Professional Engineers adopted a model "mainly directed to the development of new products, usually resulting from technological advances."[17] One can simply Google "Systems Engineering" and the references will testify to the near-universal acceptance of this process for the development of complex systems. Systems engineering, arguably, has been shown to be the most effective process for the development and operational deployment of complex systems. Although a disciplined approach and technical due diligence are central to the process, systems engineering has a proven track record for realizing progress as rapidly as possible.

During the 1990s, DOD experimented with acquisition reform, looking for ways to streamline the acquisition process, decrease the development time line, and provide more latitude for innovation to contractors. "Shortcuts" were taken in the belief that less "rigor" and "discipline"

[16] Ibid.

[17] Ibid.

may be be necessary in the acquisition process. By the turn of the century, there was significantly more insight into what worked and what did not work. In 2004, the Undersecretary of Defense for Acquisition, Technology, and Logistics [USD (AT&L)] promulgated a new policy[18] mandating the use of a robust systems engineering approach for "all programs responding to a capabilities or requirements document, regardless of acquisition category." In the words of USD (AT&L):

> "Application of a rigorous systems engineering discipline is paramount to the Department's ability to meet the challenge of developing and maintaining needed warfighting capability. ... Systems engineering provides the integrating technical processes to define and balance system performance, cost, schedule, and risk."

Guidance for implementation followed.[19]

CONSIDERATIONS FOR IMPLEMENTING THE SYSTEMS ENGINEERING METHODOLOGY

Equally as important as adopting a systems engineering methodology for developing complex systems, is the selection of an implementation strategy that ensures adherence to the principles of systems engineering, and verifies successful execution of each of its various phases. Ultimately, the Government is accountable for results, and must ensure adequate technical competence is brought to bear for understanding issues and making decisions. For developing massive, complex systems, the Government may need to engage third party organizations to support them in this capacity.

The systems engineering methodology is not prescriptive regarding implementation strategies. The roles played by

[18] Michael W. Wynne, Under Secretary of Defense (AT&L), "Policy for Systems Engineering in DOD," February 20, 2004.

[19] Glenn F. Lamartin, Director, Defense Systems USD (AT&L), "Implementing Systems Engineering Plans in DoD – Interim Guidance," March 30, 2004.

various organizations should be considered in light of how the activities in the systems engineering methodology might best be performed. For each system development activity, specific consideration should be given to enabling key roles for Government agencies and Government Laboratories, prime contractors, associate contractors, Federally Funded Research and Development Centers (FFRDCs), University Affiliated Research Centers (UARCs), academia, non-profits, and small or minority owned businesses. In architecting an implementation strategy, especially in defining the roles of prime contractors, note that history has shown that the strength of this Nation for addressing massive, complex challenges is the wealth of available domain expertise, and the power of competitive forces.

To begin with, massive, complex systems normally require major contractors because they usually have the resources for manufacturing and production that smaller businesses do not have. In addition, large organizations have infrastructure, logistics, and in-service engineering capabilities that are critical to lifecycle support. The considerable scale of the challenge in securing the borders necessitates a major contractor in the role of prime for system development and deployment.

There are many smaller companies not engaged in manufacturing and production; they necessarily rely on their subject matter expertise for providing value added to their customers. These organizations can provide critical support in assessing needs and feasibility, defining concepts, exploring operations, and providing intellectual property in understanding the problem and developing technologies. Because this is all that they do, they must be very competitive in what they provide. Therefore, one would not necessarily expect to see all the domain expertise resident in a prime contractor. To access the “best and brightest,” ways should be found to include these “associate contractors” as full members of the team.

The Nation has a significant resource in its nonprofit laboratories that can operate in the best interest of the Government as “Honest Brokers.” These organizations include Government laboratories (e.g., DOD service laboratories), the “National Labs” (DOE), Federally Funded Research and Development Centers (FFRDCs), and University Affiliated Research Centers (UARCs). The absence of shareholders, manufacturing, and production allows more independence (less conflict of interest) in supporting the Government in developing requirements, planning, prototyping, testing, and assessing operational effectiveness.

There are numerous examples of disparate successful strategies for implementing the systems engineering methodology. SSP’s management of the Polaris Program, previously mentioned, included a technical staff of 450 in the program office fully dedicated to the development and production of the Polaris system. This represents an example of a model with a strong technical role played by the Government. Two of the five major features identified by the GAO as contributing to this program’s success are:[20] “(4) program office technical expertise, and (5) good management practices, such as open communications, independent internal evaluation, and on-site management representation at contractor plants.”

A considerably different model that emerged is the recognized successful[21] spiral development strategy used by the U.S. Navy for improving submarine sonars [Acoustic Rapid Commercial Off-the-Shelf (COTS) Insertion (ARCI)/ Advanced Processor Build (APB)] starting in the mid 1990s. The Navy had made a commitment to embrace open architecture, in general, for new systems development efforts to enable a spiral development systems engineering methodology, and specifically to allow contributions from many organizations across the full spectrum of systems engineering activities. Mandating open architecture alone, while necessary, proved to be insufficient in many programs for changing the roles and contributions of organizations in the acquisition process. Progress in improving the acquisition

[20] United States General Accounting Office, “Fleet Ballistic Missile Program,” GAO/NSIAD-90-160, 9-6-1990.

[21] Winner of the Al Gore “Hammer Award for Reinventing Government” in February, 1999.

process, had, in fact, been hampered by the continued use of traditional business practices that limit intellectual competition. In the words of the Chief of Naval Operations (CNO):[22] "Although we have made considerable Open Architecture (OA) investments over the past several years, we have been holding onto traditional business models and the overall progress transitioning into OA business practices is disappointing." The CNO then cites the ARCI/APB program, as an exception, for its successful business model: "It (ARCI/APB) provides a clear and compelling example of competitive alternatives bringing reduced costs, improved capability, and increased speed of delivery to the fleet."

The key aspect of the ARCI/APB business model cited by the CNO is how organizational roles are carefully tailored (Figure 2) to address the elements of systems engineering.

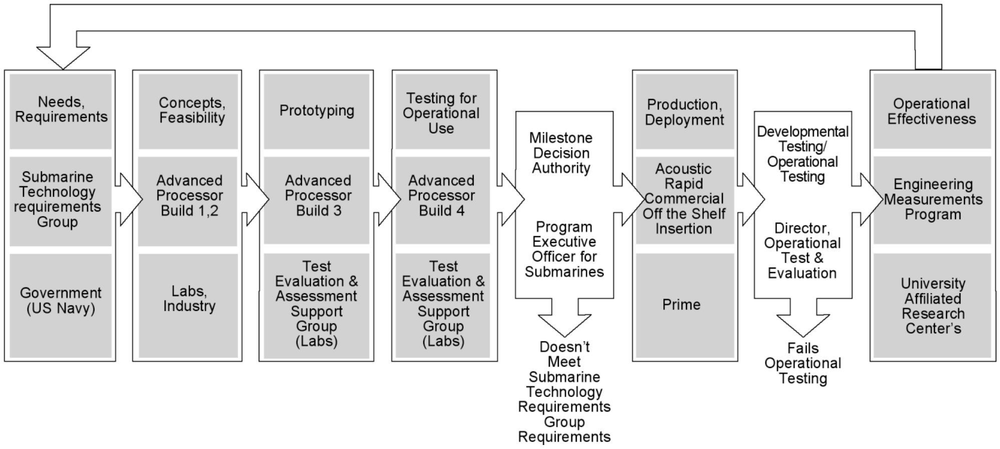
Needs, Requirements
Submarine Technology requirements Group
Government (US Navy)
Concepts, Feasibility
Advanced Processor Build 1,2
Labs, Industry
Prototyping
Advanced Processor Build 3
Test Evaluation & Assessment Support Group (Labs)
Testing for Operational Use
Advanced Processor Build 4
Test Evaluation & Assessment Support Group (Labs)
Milestone Decision Authority
Program Executive Officer for Submarines
Doesn't Meet Submarine Technology Requirements Group Requirements
Production, Deployment
Acoustic Rapid Commercial Off the Shelf Insertion
Prime
Developmental Testing/ Operational Testing
Director, Operational Test & Evaluation
Fails Operational Testing
Operational Effectiveness
Engineering Measurements Program
University Affiliated Research Center's

Figure 2 The systems engineering methodology related to key aspects of the Navy's ARCI/APB business model.

Requirements are set by a requirements group composed of Government (U.S. Navy) users. These are updated based on measured performance and changes to the threat. The broad scientific community, in general, supports the identification of concepts and assessment of feasibility. The Laboratory community develops prototypes, and as a group of peers

[22] M.G. Mullen, Chief of Naval Operations, "Navy Open Architecture," Department of the Navy, August 28, 2006.

[Test, Evaluation, and Support Group (TEASG)] assesses suitability of the concept for operational use. The results of this testing are used by Program Executive Office (PEO) Subs (Milestone Decision Authority) to validate that requirements are met before production. The Prime Contractor produces and deploys the system, and the Government [Director of Operations, Test and Evaluation (DOT&E)] verifies operational performance. During operational patrols, the Labs continuously assess operational effectiveness, and feed back results to the process to continue spiral development. Organizations do what they do best, conflicts of interest are minimized, and intellectual competition is encouraged throughout the process.[23] In the words of the CNO: "My vision for OA is not limited to systems built to a set of open standards, but rather it is focused on open business models for the acquisition and spiral development of new systems that enable multiple developers to collectively and competitively participate in cost-effective and innovative capability delivery to the Naval Enterprise."

One other basic aspect of the systems engineering implementation used by the ARCI/APB program must be mentioned because of its significance for ensuring real and rapid progress. Every concept/design/improvement is subjected to data-driven evaluation or assessment at every phase of the process to establish maturity, understand risk of implementation, and determine value added to overall performance. Key elements of this strategy are models validated with data, common data sets (real data) and common metrics, end-to-end test beds, in-situ testing, and peer review teams. This represents an example of a model that exploits the greater technical community to a very considerable extent.

Achieving Rapid Progress

Given the urgency of the current national security environment, a crucial issue for any methodology and any

[23] An unnamed staff member of the prime contractor for ARCI found competition after contract award intellectually stimulating: "I wouldn't want to go back to the old way."

implementation strategy is “How rapidly can one make progress?” If it takes too long to get to the 100% solution, one might be willing to take a 90% or 80% solution in the short term. (Or as a worst case, one might pursue activities rapidly that consume resources and time and result in no real progress.)

Begin by recognizing that there is no magic process that can guarantee an arbitrary degree of progress in an arbitrarily short amount of time—even by throwing money at the problem. Then recognize that the systems engineering methodology, properly implemented, has the proven track record for realizing real progress as rapidly as possible. Very importantly, the systems engineering methodology can be tailored to emphasize milestone-driven development. In the ARCI program mentioned previously, the “R” stands for “Rapid.” Whereas, the traditional acquisition process for submarine sonars took 12 or more years to develop and implement improvements, the ARCI/APB spiral development process deploys a new build for sonars every year. Properly applying a systems engineering methodology to the border security challenge would seemingly offer the highest likelihood of progress as rapidly as possible. Moreover, a spiral development process for the border security challenge could reasonably produce yearly improvements in real performance.

The ARCI/APB program, initiated in 1996, deployed its first version at sea in 1998 – two years. Lessons from successful spiral development programs shed light on what it takes to make rapid progress at the initiation of a program:

- Major hardware systems and infrastructure take time to develop. The more that exists, the faster progress can be made at the beginning.
- Open Architecture and COTS systems are key enablers for rapidly inserting software upgrades, and allowing any organization to “plug and play”.
- Contracting can easily delay progress. Multiyear contracting with key organizations, IDIQ contracts, and appropriate use of sole source contracting can all help.

- Technology that leads to performance improvements needs to be "in the pipeline," and the implementation strategy should ensure accessibility to this technology, wherever it might exist in the greater technical community.
- The Government needs a key individual (Program Manager) empowered to do the right things – and it helps if he or she is a zealot.

RECOMMENDATIONS

The following recommendations address the scope and complexity of the border security challenge, the impact of initial policy and requirements development with clear, holistic metrics, and proven implementation strategies.

- Recognizing the massive scale and complexity of the border security challenge, a firm commitment needs to be made to a disciplined systems engineering methodology for controlling performance, cost, and schedule and for providing the oversight tools the Government needs for monitoring performance and ensuring success.

Even with SBInet prime contractor selection by September 30, 2006, the systems engineering methodology can still be applied during rapid development and deployment to support operational success.

- Policy, goals, metrics, and requirements must be defined at the beginning.

CONOPS, policy, goals, metrics, and requirements for SBInet should be clearly articulated to the prime early in the development process. An integrated view must be developed for the roles of federal, state, and local agencies.

- An implementation strategy should consider enabling multiple organizations to collectively and competitively participate in all elements of system design, development, and deployment.

Organizational constructs for SBInet that vest too much responsibility and authority in a single prime organization may diminish objectivity and alternatives, and fail to exploit the Nation's strengths for solving its challenges – a *wealth of technical resources, and an open competitive market for ideas.*

- Organizational conflict of interest must be avoided in testing and evaluation by using Government, nonprofit, and peer review organizations.

The Nation's nonprofit laboratories (e.g., DOD Labs, the DOE "National Labs," FFRDCs, and UARCs) operate for the Government as "Honest Brokers." The absence of shareholders, manufacturing, and production in these organizations provides the Government an opportunity for independent validation and oversight of SBInet. In particular, the Nation's nonprofit Labs can support requirements development, planning, prototyping, testing, and assessment of operational effectiveness.

- Technology development and validation, risk reduction, testing for operational effectiveness, prototyping, limited production, and deployment – should all be performed before full-scale production and deployment.

A scaled prototype of an integrated system for SBInet should be developed and tested in an operational environment with border patrol agents. Full-scale production and deployment should begin only after discrepancies are resolved, and operators accept the system.

- A continuing assessment of operational performance – determination of deficiencies, issues, and lessons learned – should feed back into a spiral development process for developing improved technologies and operations and improving performance.

Given the lack of maturity in the marriage of technology and operations that support the border security mission area, a "spiral development" process should be used that exploits continually developing knowledge in this domain, adapts to technology improvements, and continually refines the CONOPS and tactical operations.

- Given the urgency of today's national security environment, DHS should take those actions necessary to ensure real and rapid progress in the near-term.

Secretary Chertoff has stated that SBI/SBInet will make significant progress in two years.[24] *What could SBInet reasonably attempt to accomplish in that time? The current ISIS sensors, remote video surveillance, and existing infrastructure, and an imminent multiyear, IDIQ prime contract are significant resources for getting started. Importantly, there exist key technologies in the pipeline that apply to SBInet's most critical issues: e.g., false alarm reduction algorithms, "large margin" classifiers, bell ringers, automatic target recognition, data fusion algorithms, and tactical scene generation. The data stream from existing sensors could be employed immediately for providing critical inputs to "data driven" research and development of these new technologies. These technologies, however, exist at many different organizations, and typically, outside the DHS community. So, the organizational implementation strategy used for SBInet should accommodate—even encourage—outreach to a broad technical community. Moreover, an open architecture should be used for system development and implementation to allow any organization to "plug and play." Properly constructed and managed, in two years SBInet could meaningfully attempt deployment of a limited prototype that demonstrates orders of magnitude improvement in critical performance areas (e.g., false alarm reduction), successful resolution of critical technical issues, and a baseline system that enables full-scale development and deployment.*

CLOSING

Again, I thank you for this opportunity to address you today on "How Can Technologies Help Secure Our Borders?," and specifically how applying the discipline of

[24] Oral Testimony by Secretary Michael Chertoff, before the U.S. House of Representatives Appropriations Subcommittee on Homeland Security, Rayburn House Office Building, July 27, 2006, reported by UPI on July 28, 2006: *Chertoff Pledges Better Border Security,* by Martin Sieff.

the systems engineering methodology can ensure that Congress' investment in SBI and SBInet will be rewarded with operational success. This ends my remarks concerning the applicability of a disciplined systems engineering approach to the daunting challenge of securing our Nation's borders.

BIOGRAPHY

Gordon Daniel Tyler
Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road, Laurel, MD 20723
240-228-5032

Company Title(s): Department Head, National Security Technology Department

Business Area Head for Undersea Warfare
Business Area Head for Homeland Protection
Business Area Head for Biomedicine
Member APL Executive Council

Areas of Practice/Specialization:

With 36 years experience in research, development, test and evaluation, Mr. Tyler has been in technical, program management, and line management positions. He has supported DOD, the Intelligence Community, the Department of Homeland Security, and other Government agencies in various mission areas, including Undersea Warfare (Submarine Security, Anti-Submarine Warfare), Homeland Security/Homeland Defense (Maritime Domain Awareness, Border Protection, Counterdrug, Infrastructure Protection, Preparedness and Response), and Special Operations. His areas of technical specialization include: Sensor and System Development; System Concept Development and System Engineering; Operations Analysis, Modeling and Simulation, and Test and Evaluation.

Honors, Degrees:

M.S., Johns Hopkins University, 1974, Computer Science
B.S., Massachusetts Institute of Technology, 1970, Electrical Engineering
Stanford Executive Program, Graduate School of Business, Stanford University, 2002
Merle Tuve Fellowship (1985)
Doctoral Coursework, Johns Hopkins University (1978-1985), Applied Mathematics

Work Experience:

1970 – Present: Johns Hopkins University Applied Physics Laboratory

Department Head, National Security Technology Department **1998 – Present**

Head line manager for APL department of 525 staff responsible for activities in Homeland Protection, Undersea Warfare, and Biomedicine, with principal organizational competencies in physics, sensors, signal and information processing, system concept development and systems engineering, test and evaluation.

Business Area Head for Homeland Protection

1998 – Present

Responsible for APL business activities in Homeland Security/Homeland Defense (180 staff years of effort), which includes the following thrusts:

- Preparedness and Response: Syndromic Surveillance/Biosurveillance/ESSENCE, for DARPA, DTRA, CDC, NCR; regional response planning, “first responder” support, and operational response T&E for DHS, NIH, MD;
- Key Facilities Protection: Mail screening and mail security activities for the US Government and DOD; CBRNE sensor evaluations, pentagon security for PFPA;
- Maritime and Border Security: Portal Systems T&E for TSA; Container and In-Bond Security for C&BP; Advanced Spectral Systems for DNDO; Maritime Domain Awareness and Maritime Security for USCG;
- Special Operations and ISR: Systems engineering and analysis for SOCOM; Ops assessments and gaps evaluation for JIEDDO; special ISR projects for the intelligence community; systems engineering and analysis support for the Naval Special Warfare Development Group;
- CBRNE Detection and Defeat: CBRNE sensor/system RDT&E for JPEO CBD; sensor T&E and performance analysis for JPEO CBD; Spectral Sensing for Bioaerosols for DARPA; “gold standard”

testing for HSARPA; systems engineering and analysis support for DTRA.

Business Area Head for Undersea Warfare **1998 – Present**
Responsible for APL business activities in Undersea Warfare (350 staff years of effort) which includes the following thrusts:

- Submarine Security and Technology: SSBN Security Program; Submarine Security and Survivability Program;
- Anti-Submarine Warfare: Advanced Processor Builds for Submarine Sonar, Tactical Control, and Surface Ship Sonar; Engineering Measurements Program for Submarine Sonar (T&E); numerous ONR S&T efforts; Integrated Undersea Surveillance Systems; numerous special studies, analyses, and war games that directly support the office of the CNO.
- USW GWOT activities: Submarine In-Port and Near-Port Security; Nuclear Weapons Security; Pearl Harbor Port Security (NFESC);

Principal sponsors in Undersea Warfare include Director of Submarine Warfare (CNO N87); PEO Integrated Warfare Systems; NAVSEA; NAVAIR; SPAWAR; ONR; Strategic Systems Project Office; DARPA.

Business Area Head for Biomedicine **1998 – Present**
Responsible for APL business activities in Biomedicine, which includes the following efforts:

- A revolutionary 22 degree of freedom upper extremity prosthetic with full neural integration (peripheral nerves, cortical neurons), and haptic feedback (DARPA); APL lead for team of world-wide, expert organizations; APL responsible for system engineering and integration;
- Biomechanics: Blunt trauma modeling and testing; Head-Supported Mass Program for the US Army; vehicle and occupant response to IED detonation; Crash Test Facility testing.

<u>NSTD Assistant Department Head for Programs</u> 1994 – 1998
Department supervisor responsible for program management and development activities including: fiscal year/multiyear planning; identification and development of strategic thrust areas; system concept development; program/project formulation; coordination and monitoring of program activities; identification of fiscal, human, and capital resources required to execute program activities; development of teaming arrangements with industry, academia, and government labs. The principal areas addressed consist of: Undersea Warfare technologies and systems (Submarine Security, Surveillance, Anti-Submarine Warfare, Mine Warfare); Information Science and Technology (Simulation, Modeling, Data Integration and Fusion, Signal and Information Processing, C^3I, Intelligent Networking); Marine Engineering, Test and Evaluation; Counter-Drug technologies and systems; Ocean and Atmospheric Physics; technologies and systems for countering weapons of mass destruction; and Healthcare Technologies.

<u>Undersea Surveillance Program Area Manager</u>   1988 - 1994
Responsible for the development and management of Undersea Surveillance and Anti-Submarine Warfare systems and technologies, including: directed research, basic science and technology development; system engineering (requirements definition; modeling, simulation and analysis; system concept development; prototyping; system engineering and integration; test and evaluation; system architecture development; C^3I; operational evaluation); concept of operations development. Major programs included: Integrated Undersea Surveillance Systems programs (Low Frequency Active, Critical Sea Test (Lead Lab), Air Defense Initiative, SURTASS development (Lead Lab), Advanced Distributed Systems, Full Spectrum Processing); avionics for the LAMPS helo program; BEARTRAP; Periscope Detection Radar; and DARPA simulation and modeling development.

Acoustics Program Manager for the SSBN Security Technology Program **1981 – 1987**
Responsible for 8 to 10 projects in the SSBN Security Program investigating the underwater acoustic detection of submarines. Projects emphasized basic physics, modeling, simulation, signal and information processing, system concept formulation, system design and engineering, test and evaluation, and operations analysis. Projects included: radiated signatures of submarines; mobile, low frequency active acoustic systems (DIANA, Standard Aura I, II, and III); fixed, low frequency active systems (Fixed-Fixed I, II, III); sub-on-sub operations (Standard Arrow I, II); exploitation of transient and intermittent acoustic radiation (LANTSECEX and PACSECEX testing); and sonar performance in oceanographic ducting conditions.

Advanced Concepts Section Supervisor of the Acoustics Group **1976 – 1980**
Line supervisor responsible for the development and evaluation of advanced underwater acoustic technology and system concepts for the detection of submarines. The scope of activities included: identification of key technologies; development of operational concepts; performance of scoping calculations with performance models; identification of critical issues and the conduct of analytical or experimental efforts for resolution.

Assistant Program Element Manager of the Acoustics Group **1979 – 1980**
Assistant Program Manager for the acoustics projects in the SSBN Security Program. Supported the Program Manager in planning, executing, and monitoring major acoustics projects including Standard Argo (exploitation of acoustic noise field anisotropy with high resolution sonar arrays), LANTSECEX 302-80 (detectability of specific signature components in acoustic surface ducts), and special analyses of Sonar Evaluation Program data.

Project Leader for SSBN Security Program Efforts: **1976 – 1980**

- Standard Aries Sea Test and Analysis: Exploitation of underwater acoustic surface ducting conditions for submarine detection. Directed project team performing environmental surveys and test area selection, pre-test performance predictions, test geometry designs, identification of critical issues associated with physics of acoustic propagation and scattering, measurement designs, signal processing, and overall analysis plans.

- Advanced Concepts Analysis Project: Directed team of analysts investigating advanced acoustic concepts for submarine detection as part of the SSBN Security Program. Specific concepts included interarray processing (IAP), low frequency active acoustic sonars, planar arrays, distributed sensors, oceanographic exploitation, and the utilization of loud, intermittent acoustic evolutions.
- Skeleton Array Exercise (SKELEX): Principal analyst and Project team lead, for planning, conducting, and performing analysis for the SKELEX at-sea exercise addressing maximum achievable gains for passive sonar towed arrays.

Associate Engineer, Acoustics Group **1970 – 1976**
Designed and developed digital signal processing hardware, algorithms, and software in support of analysis of underwater acoustics data, for assessing sonar performance in support of the SSBN Security Program. Designed and developed high-speed programmable array processor. Designed and implemented high-speed frequency domain algorithms for correlation, beamforming, and automated detection. Principal investigator for infrasonic detection of submarines, surface scattering effects on sonar performance, and Interarray Processing.

Publications:

The Emergence of Low Frequency Active Acoustics as a Critical Anti-Submarine Warfare Technology, Johns Hopkins APL Technical Digest, Vol. 13, No. 1, 1992.
An Overview of the Critical Sea Test Program, US Navy journal of Underwater Acoustics, Vol. 42, No. 2, 1992.
Array Signal Gain Measurements for a Large Aperture Acoustic Array Operating in a Convergence Zone Environment, Proc. 32nd Navy Symposium on Underwater Acoustics,1978.
Measurement of Signal Coherence, Propagation, and Array Dynamics with a Large Acoustic Array, APL/JHU POR-3143, April, 1976.

Associations:

Naval Submarine League
National Defense Industrial Association
Armed Forces Communications and Electronics Association